Before the
FEDERAL COMMUNICATIONS COMISSION
Washington, D.C. 20554

In the Matter of	)	
	)	
Promoting Technological Solutions to Combat Contraband Wireless Device Use in Correctional Facilities	)	GN Docket No. 13-111
	)	

To: The Commission

REPLY COMMENTS OF TRIPLE DRAGON – U.S., INC.

James Arden Barnett, Jr
Venable LLP
575 7th Street, NW
Washington, D.C. 20004

Attorney for Triple Dragon – U.S., Inc.

Dorothy E. Cukier, Esq.
Executive Vice President and Corporate Counsel
Triple Dragon – U.S., Inc.

Before the
FEDERAL COMMUNICATIONS COMISSION
Washington, D.C. 20554

In the Matter of	)	
	)	
Promoting Technological Solutions to Combat Contraband Wireless Device Use in Correctional Facilities	)	GN Docket No. 13-111

REPLY COMMENTS OF TRIPLE DRAGON – U.S., INC.

Triple Dragon – U.S., Inc., by its counsel, respectfully submits these reply comments in response to the Federal Communications Commission's ("FCC" or "Commission") Notice of Proposed Rulemaking ("NPRM") in the above-captioned docket. The Commission seeks assistance in the crafting of rules to foster the availability and deployment of technological solutions to combat the proliferation of wireless devices inside correctional facilities.

I. STATEMENT OF INTEREST

Triple Dragon – U.S., Inc. ("TD") is a wholly-owned, separate, Delaware-incorporated subsidiary of Triple Dragon Communications Inc. ("Dragon"), a Canadian corporation with its headquarters in Montreal, Canada. Dragon and TD provide software-based security services, including counter-incendiary explosive device defeat and suspect communications pattern analysis, domestically and internationally. TD and Dragon additionally offer an alternative to managed access service ("MAS") that neither utilizes nor impacts radio frequencies, and it is deployed and operated remotely from client premises, eliminating the need for any on-premise hardware installation. The technology is software-as-a-service, so its use is invisible and virtually impervious to defeat or tampering, and can be made available at approximately one-third the cost of MAS.

II. BACKGROUND

TD applauds the Commission for taking action on this critical issue in a rulemaking proceeding. After the FCC's workshop on contraband cell phones in prisons on September 30, 2010, criminal activity using contraband cell phones inside correctional facilities has continued and arguably has gotten worse. The illicit use of unmonitored wireless devices by inmates must be swiftly addressed by the FCC, especially now that the Cell Phone Contraband Act of 2010 has made it illegal for a federal inmate to possess a cell phone and to provide a cell phone to an inmate.[1]

[1] Cell Phone Contraband Act of 2010, Pub. L. 111-225 (enacted Aug. 10, 2010.)

TD provides an innovative, cost-effective network based solution to locate and facilitate the disabling of contraband cell phones. Its system does not impact or emit radio frequencies in TD's operations. (Consequently TD has no comment on the topic of streamlining spectrum leasing). TD is able to detect and locate precisely the contraband cell phones within the boundaries of the prison. TD's system then allows the prison warden to transmit the evidence of the location of the contraband cell phone to the carrier with the request that the phone be disabled without physical intervention. TD can do so for a fraction of the cost of managed access systems and detections systems which require the installation of hardware in the prison.

TD appreciates the concerns of the wireless industry about disabling its cell phones. However, TD maintains that the carriers will not be liable for deprovisioning cell phones under FCC regulations using a process and system such as TD's, regulations that are necessary and justified under the Communications Act of 1934 (the "Act").

III. DEPROVISIONING CONTRABAND WIRELESS DEVICES

Federal and state laws have emerged nationwide to prohibit the presence of wireless devices inside correctional facilities, certainly with respect to inmate and visitor possession, and in many cases, possession by correctional facility personnel. Wardens and commissioners of these facilities are responsible for ensuring the safety and security of all persons inside the facility (inmates and staff) and for ensuring that their inmates do no harm to the public outside the facilities. The responsibility of these prison officials aligns with the FCC's statutory purpose of "promoting the safety of life and property through the use of wire and radio communications" when it comes to defeating contraband cell phones.[2]

A. AUTHORITY FOR THE DEPROVISIONING REQUEST

The Commission proposes that authorized correctional facility officials be permitted to request commercial mobile radio service ("CMRS") to terminate service to unauthorized wireless devices.[3] AT&T notes that the Commission is incapable of simply sanctioning this, pursuant to its restricted powers of delegation of authority under 47 U.S.C. 155(c)(1).[4] CTIA-The Wireless Association ("CTIA") expresses concern that if such authority is delegated to prison officials, carriers would be required to act on termination requests from non-sworn law

[2] Communications Act of 1934, 47 U.S.C. §151.
[3] *In re* Promoting Technological Solutions to Combat Contraband Wireless Device Use in Correctional Facilities, *Notice of Proposed Rulemaking*, GN Docket No. 13-111 ("NPRM"), FCC 13-58, rel. May 1, 2013, at ¶ 65.
[4] AT&T, Comments at p. 8.

enforcement officials operating privately-owned correctional facilities.[5] Verizon does not address the issue of whether or not a prison official has the authority to order the deprovisioning of a wireless device; it advocates directly for the requirement of a court order before it will terminate wireless device service.

On the face of the law and regulations, it appears that only the FCC or a wireless carrier can carry out the act of terminating service. However, there are no statutory limitations on who can *request* termination. In a correctional facility setting, it is the warden and/or commissioner who is responsible for the day-to-day security of the correctional environment and therefore, these local law enforcement officials are the persons most capable of determining whether or not an item is contraband. While a warden or commissioner cannot unilaterally terminate service to a wireless device, his or her request to a carrier, accompanied by the best-supporting evidence available, should suffice to have that request fulfilled.

Title 47 U.S.C. §303 provides the FCC with authority to require wireless carriers to terminate service to contraband wireless devices in its express ability to "prescribe the nature of the service to be rendered by each class of licensed station and each station within any class."[6] When read together with the "authority to establish areas or zones to be served by any station," the Commission can adopt regulations requiring CMRS licensees to terminate services to contraband wireless devices in the areas under the responsibility of a prison warden.[7] In doing so, the Commission does not touch upon the matter of delegation; the carrier is required to act upon the request of the authorized prison official.

Time is always a critical factor in public safety, and in this case technology already exists for quick action. However, CellAntenna proposes that termination requests be fulfilled within two weeks of receipt.[8] Verizon advocates for termination pursuant only to court order.[9] AT&T, in the absence of a court order, would like to make the decision to terminate on its own.[10]

CellAntenna is too generous in proposing a two-week window during which inmates may continue to use the contraband cell phone to the detriment of public safety. CTIA urges the Commission to undertake a revision of

[5] CTIA, Comments at p. 10.
[6] 47 U.S.C. §303(b).
[7] 47 U.S.C. §303(h).
[8] CellAntenna, Comments at p. 3.
[9] Verizon, Comments at 10.
[10] AT&T, Comments at p. 9.

Part 2 of the rules to accommodate a new equipment certification process for detection systems.[11] It is understandable that wireless carriers would want as much time as possible to respond to a request to terminate service; however, the Commission must weigh their desire for administrative process (on behalf of a "customer" that may be breaking the law without the carrier's knowledge) against the continuing danger of contraband cell phones and the fact that technology exists to detect and verify location within a prison and provide a formatted, authorized request for termination to the carrier within minutes of detection. TD's system, for example, reduces the administrative time required of the carriers.

It is important to bear in mind that this a critical, time-sensitive public safety concern. The determination of how long a contraband wireless device should be permitted to remain operational belongs squarely with the prison official in charge of the security of his or her facility. While some facilities may prefer to detect and locate an unauthorized wireless device, and monitor its ongoing use for investigative purposes, the majority of correctional facilities simply want these devices instantly and permanently disabled. Short of legalizing jamming, immediate service termination is what wardens and commissioners want and need for public safety.

C. CARRIERS CAN RESPOND WITHOUT LEGAL LIABILITY

Carriers will not be liable for responsibly fulfilling the request of a governmental official, acting within the official's authority, to disable a cell phone which under the Contraband Cell Act (or state statute) is determined to be contraband *a priori* due to its presence in a prison.[12] Wardens and commissioners, given clear and accurate information about wireless devices in their restricted areas, are the best-positioned persons to determine whether or not a wireless device is contraband and should be disabled. Solution providers with TD's capability can present clear and accurate information to the prison official. The carrier merely responds to the warden, acting in her or his official capacity.

The Act provides that carriers may take action "to protect the rights and property of the carrier" and that location information and other customer proprietary network information (CPNI) can be used to protect its customers and the carrier itself from "fraudulent, abusive, or unlawful use of, or subscription to, such services."[13] Upon being informed of the presence of an unlawful device on the carrier's network, the exact cell phone number,

[11] CTIA, Comments at p. 8.
[12] Cell Phone Contraband Act of 2010, Pub. L. 111-225 (enacted Aug. 10, 2010.)
[13] 47 U.S.C. §222(d)(2).

identification, and latitude and longitude within the prison, the carrier may then verify the information against its own CPNI information in the process of disabling the illegal phone.

Carriers routinely respond to law enforcement requests under the Communications Assistance to Law Enforcement Act (CALEA) which directs carriers to intercept electronic communications carried on its network "pursuant to a court order *or other lawful authorization*" (emphasis supplied).[14] Verizon tacitly invokes this provision when it propounds that it should only have to respond to a court order, but carriers are not familiar with responding to "other lawful authorization," which such a request would be. Clearly, the statute anticipates something other than just a court order in every situation. The Commission is under a statutory obligation to adopt rules necessary to implement CALEA (though this section of the statute only mentions "authorization" and not "court order").[15] It should be noted that in the past situations arising under CALEA, the term "intercept" has been used with the connotation of capturing the content of the communication. However, intercept also means to prevent, as in a missile intercepting an enemy aircraft, or in this case, preventing illegal communications through a contraband cell phone.

While the Commission is obligated to effectuate the Communications Act of 1934, it cannot do so in isolation of other statutes. When the Act, CALEA and the Cell Phone Contraband Act of 2010 are read together, a responsibility emerges to ensure that contraband cell phones are not allowed to be the source of continuing criminality and public danger.

Moreover, the carriers would have the affirmative defenses of statutory compliance in the case of any claim by a non-prisoner and illegality in any claim by an inmate. The courts have long recognized that those who carry out the work of the government must have protection from liability to allow them to serve the government without undue exposure.[16] This protection is enhanced when carriers are provided with the request as well as comprehensive data upon which the request is based.

Carriers can be provided with the most incontrovertible evidence available when a service termination request is received, so that it can quickly and confidently assess the request and terminate service in good conscience. Robust, comprehensive data associated with a prison official's request to terminate wireless device service should eliminate the need to also obtain a court order, terminate phones in batches, or require a lengthy hold

[14] 47 U.S.C. §1002(a)(1) and §1004.
[15] 47 U.S.C. §229(a) and (b).
[16] *See* Filarsky v. Delia, 566 U.S. ____, 132 S.Ct. 1657 (2012)

on a request while a carrier devotes time and resources to develop its own verification that a device is being operated without authorization.

TD has the ability to send a de-activation request directly to a carrier's activation platform. Given the industry's concern that only the FCC or a relevant carrier can terminate wireless service, TD can submit a prison official's termination request in an alternative manner. Attachment A is an example of the data support that accompanies every request to terminate wireless service, which data is initially used by a prison official to make the request.

TD provides each and every carrier whose signals are operational at a correctional facility site an aerial map of the correctional facility, with the correctional facility's restricted areas (as determined by the correctional facility) demarcated in red. Before TD begins servicing the facility, the carriers know, visually and by latitude and longitude, the precise areas that are legally off-limits to wireless devices.

When a wireless device is detected, it appears as an icon on the aerial map at its location, which is determined by both cell tower triangulation and GPS (in cases where the phone is in an outdoor restricted area.) An icon of the device, when clicked with a mouse, opens a box that provides the prison official, and later the carrier, with the following information about the device:

- IMSI/IMEI/ESN/MIN
- Device name (phone number)
- Lat/long of device position
- Mode of device utilization at time of detection, *e.g.*, incoming/outgoing voice call, incoming/outgoing text message, data download/upload
- Carrier
- Device Vendor/Model

Carriers see only devices for which they provide service; devices detected within restricted areas that are serviced by other carriers are visible only to TD and the prison official. The request for service termination is accompanied by this screenshot, which provides detailed device data, and visual affirmation that a device is operating inside an area legally restricted for contraband. If the carrier complies with TD's request to send notification immediately upon service termination, a screen shot of the device at termination will be provided to the carrier for its records as support in the event of a dispute. This, in concert with the termination provisions present in

most, if not all, carrier customer service agreements, should provide carriers with defensible justification to act expeditiously when termination requests are received.

IV. CONCLUSION

TD encourages the Commission to require that CMRS providers terminate service to contraband wireless devices promptly upon a request from a prison warden, commissioner or other authorized prison official based upon clear data that shows that the cell phone is in use in violation of federal or state law or prison policy. The Commission has the authority to do so, and the carriers have the authority to respond without liability. The failure to do so perpetuates a significant, increasing and proven public safety crisis when technological solutions are available. Indeed, the carriers have shown a strong reluctance to turn off contraband cell phones in the absence of Commission regulations, even though it is within their technological capability.

TD also encourages the Commission to adopt the regulations in such a way that does not disadvantage innovative and cost-effective technologies such as TD. MAS and on-premise detection are not the only solutions and are actually more expensive and more difficult for the carriers to administer. TD's unique design, which involves zero hardware installation, no on-premise presence, and highly accurate detection and location functionality, is available at a cost that most correctional facilities can afford without subsidization. The degree of automation and compatibility with the carriers reduces the carriers' time, effort and investment in supporting the solution. TD hopes that this NPRM perpetuates momentum in the quest to provide correctional facilities with effective, affordable contraband wireless device solutions, and generates rules that are neither burdensome nor exclusionary to new, innovative solutions.

Respectfully submitted,

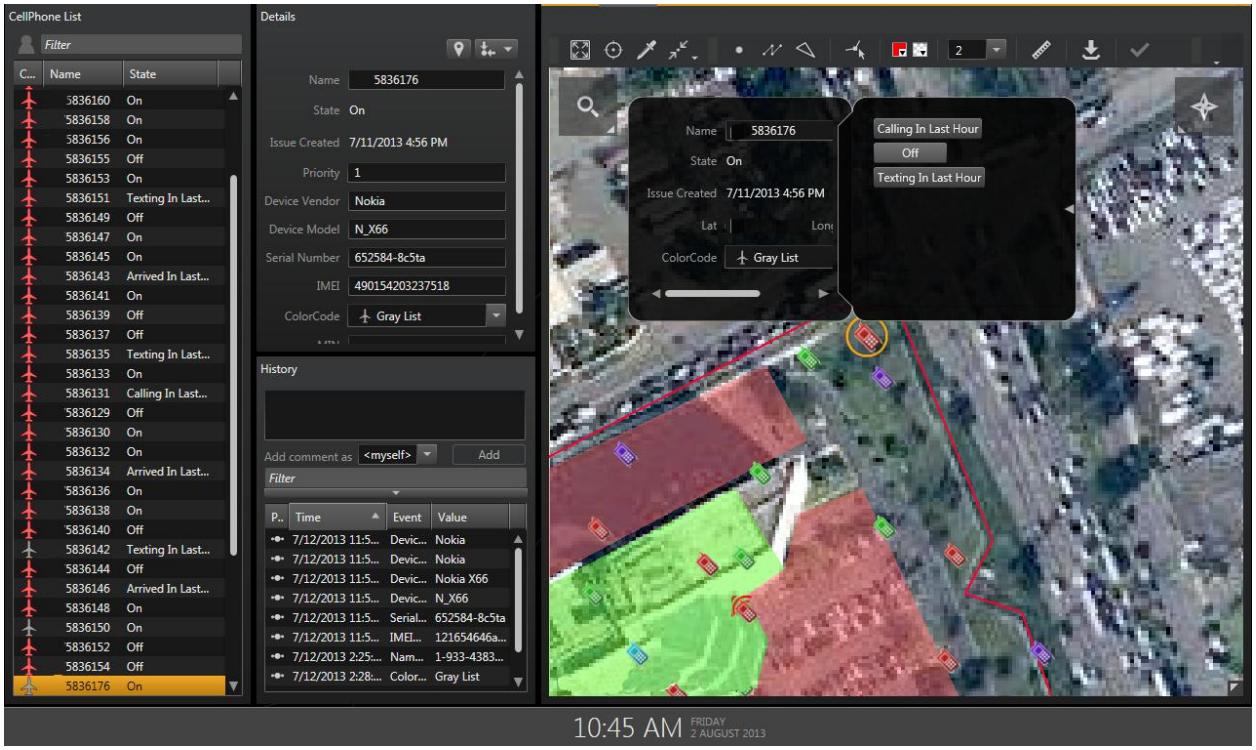
TRIPLE DRAGON – U.S., INC.

By: //s//.
James Arden Barnett, Jr.
Rear Admiral (Ret.)
Venable LLP
575 Seventh Street, N.W.
Washington, D.C. 20004
(202) 344-4695

Its Counsel

Dated: August 23, 2013

Attachment A



A "gray list" cellphone (orange circle) has been detected inside the facility. The operator can click its icon or the list on the far left for more details or to gain control of the device. The center column of the operator's display provides detailed information about the selected phone and its communications. Information about the cellphone such as its identity and location are shown on the display, allowing the operator to use the slide-out menu to review the device detail to decide the next action – to monitor or terminate service.

CERTIFICATE OF SERVICE

I hereby certify that on this 23d day of August, 2013, a true and correct copy of the foregoing document was served by electronic service on the following:

Chairwoman Mignon Clyburn
Federal Communications Commission
Attn: Louis Peraertz, Legal Advisor
Louis.Peraertz@fcc.gov

Commissioner Jessica Rosenworcel
Federal Communications Commission
Attn: David Goldman, Senior Legal Advisor
David.Goldman@fcc.gov

Commissioner Ajit Pai
Federal Communications Commission
Attn: Courtney Reinhard, Legal Advisor
Courtney.Reinhard@fcc.gov

David Turetsky, Chief
Public Safety and Homeland Security Bureau
Federal Communications Commission
David.Turetsky@fcc.gov

David Furth, Deputy Chief
Public Safety and Homeland Security Bureau
Federal Communications Commission
David.Furth@fcc.gov

Timothy May
Communications Specialist
Public Safety and Homeland Security Bureau
Federal Communications Commission
Timothy.May@fcc.gov

Ruth Milkman, Chief
Wireless Telecommunications Bureau
Federal Communications Commission
Ruth.Milkman@fcc.gov

James Schlichting, Senior Deputy Bureau Chief
Wireless Telecommunications Bureau
Federal Communications Commission
James.Schlichting@fcc.gov

John Leibovitz, Deputy Bureau Chief
Wireless Telecommunications Bureau
Federal Communications Commission
John.Leibovitz@fcc.gov

Jane Jackson, Associate Bureau Chief
Wireless Telecommunications Bureau
Federal Communications Commission
Jane.Jackson@fcc.gov

Charles Mathias, Associate Bureau Chief
Wireless Telecommunications Bureau
Federal Communications Commission
Charles.Mathias@fcc.gov

//s//
James Arden Barnett, Jr.